

On the Capacity of the One-Bit Deletion and Duplication Channel

Hamed Mirghasemi and Aslan Tchamkerten

Abstract—The one-bit deletion and duplication channel is investigated. An input to this channel consists of a block of $\ell \geq 1$ bits which experiences a deletion with probability p , a duplication with probability q , and remains unchanged with probability $1 - p - q$. For this channel a capacity expression is obtained in the asymptotic regime where $p + q = o(1/\log \ell)$. As a corollary, we obtain an asymptotic expression for the capacity of the so called “segmented” deletion and duplication channel where the input now consists of several blocks and each block independently experiences either a deletion, or a duplication, or remains unchanged.

I. INTRODUCTION

Given an integer $\ell \geq 1$ and two constants $p, q \in [0, 1]$ such that $p + q \leq 1$, the segmented deletion and duplication channel treats independently each consecutive length ℓ binary input block in one of the following ways:

- one bit is deleted with probability p ,
- one bit is duplicated with probability q ,
- the block remains unchanged with probability $1 - p - q$.

Conditioned on a bit being deleted (duplicated) in a particular block, the deletion (duplication) occurs randomly and uniformly over the block. Hence, the unconditional probability that any particular bit is deleted or duplicated is equal to p/ℓ and q/ℓ , respectively.

When $\ell = 1$, the segmented deletion and duplication channel becomes the standard deletion and duplication channel where each input bit is independently deleted with probability p , duplicated with probability q , and is left unchanged with probability of $1 - q - p$.¹

An input to the channel consists of $s \geq 1$ consecutive blocks of length ℓ . The corresponding output is thus a binary string of known length between $n - s$ and $n + s$ where

$$n \stackrel{\text{def}}{=} s \cdot \ell.$$

Rate R is said to be achievable if, for any $\varepsilon > 0$ and s large enough, there exist 2^{nR} codewords and a decoder whose average error probability over codewords is no larger than ε . Capacity is the supremum of achievable rates and admits the

This work was supported in part by an Excellence Chair Grant from the French National Research Agency (ACE project). H. Mirghasemi and A. Tchamkerten are with the Communications and Electronics Department, Telecom ParisTech, 75634 Paris Cedex 13. Email: {mirghasemi, aslan.tchamkerten}@telecom-paristech.fr.

¹See, e.g., [1], [3], [6], [8], [11], [13] for recent references on the i.i.d. deletion and duplication channel.

asymptotic expression

$$C = \lim_{s \rightarrow \infty} \frac{1}{n} \max_{X^n} I(X^n; \mathbf{Y}(X^n)) \quad (1)$$

according to Dobrushin’s capacity theorem [2, Theorem 1].

Segmented channels with synchronization errors were introduced by Liu and Mitzenmacher in [9] where, following an algorithmic approach, they proposed a zero-error coding scheme and thereby established a numerical lower bound on the capacity of the segmented deletion channel (*i.e.*, for $q = 0$).

A difficulty in obtaining a tight single-letter characterization of C stems from the fact that the receiver does not know the error pattern, *i.e.*, which out of the s blocks experienced a deletion or a duplication (albeit it knows the overall number of deletions and duplications). As a consequence, errors “propagate” across blocks.

A useful technique to derive upper and lower bounds on C is to reveal the receiver the error pattern $E^s = \{E_i\}_{i=1}^s$ where $E_i = -1$ if the i -th block experienced a deletion, $E_i = 1$ if the i -th block experienced a duplication, and $E_i = 0$ otherwise [4], [14]. When this side information is provided to the receiver, each block can be considered in complete isolation and we obtain the so-called “one-bit” deletion and duplication channel. The capacity C_{SI} of the one-bit deletion and duplication channel is the capacity with respect to a single length ℓ block. We hence have the obvious upper bound

$$C \leq C_{SI}, \quad (2)$$

where

$$C_{SI} = \frac{1}{\ell} \max_{X^\ell} I(X^\ell; \mathbf{Y}(X^\ell)), \quad (3)$$

where X^ℓ denotes a random input block to the channel, and where $\mathbf{Y}(X^\ell)$ denotes the corresponding output.

A lower bound to C in terms of C_{SI} can be obtained by using the argument of [14, Section II.C]. First observe that

$$I(X^n; \mathbf{Y}(X^n), E^s) \leq I(X^n; \mathbf{Y}(X^n)) + H(E^s).$$

Using that $H(E^s) = sH_b(p, q)$ where $H_b(p, q)$ denotes² the entropy function $-p \log p - q \log q - (1 - p - q) \log (1 - p - q)$, it then follows that

$$C_{SI} - \frac{1}{\ell} H_b(p, q) \leq C. \quad (4)$$

²Logarithms are taken to the base 2 throughout the paper.

Note that an analytical expression for C_{SI} remains to be found and a numerical evaluation, for instance, via the Arimoto-Blahut algorithm, is computationally heavy already for moderate values of ℓ , say $\ell \geq 17$.

In this paper, we provide analytical upper and lower bounds on C_{SI} which, via (2) and (4), yield upper and lower bounds on C . These bounds are tight in certain asymptotic regimes yielding the main capacity results.

Throughout the paper, the following notational conventions are adopted. A binary length n vector is usually denoted by a bold script, *e.g.*, \mathbf{x} , and its length is denoted by $|\mathbf{x}|$. If we want to emphasize the length of a vector, we alternatively write x^n . For computational convenience, we sometimes refer to a particular sequence \mathbf{x} using its runlength description $\mathbf{r}(\mathbf{x}) = (x_1, \{r_i(\mathbf{x})\})$ where $r_i(\mathbf{x})$ denotes its i th runlength.³ For instance, the runlength description of 0100110 is (0, 11221).

We use $\mathbf{y} \prec \mathbf{x}$ whenever \mathbf{y} is a subsequence of \mathbf{x} , *i.e.*, whenever \mathbf{y} results from the deletions of $|\mathbf{x}| - |\mathbf{y}|$ bits of \mathbf{x} .

The next section contains our main results and Section III is devoted to the proofs.

II. MAIN RESULTS

Let

$$L_{SI}^\alpha \stackrel{\text{def}}{=} \frac{I(X^\ell(\alpha); \mathbf{Y}(X^\ell(\alpha)))}{\ell} \quad (5)$$

where $X^\ell(\alpha) = X_1, X_2, \dots, X_\ell$ refers to the Markovian input given by

$$\begin{aligned} Pr(X_1 = 0) &= Pr(X_1 = 1) = \frac{1}{2} \\ Pr(X_i \neq X_{i-1}) &= \alpha, \quad 2 \leq i \leq \ell, \end{aligned} \quad (6)$$

for some fixed parameter $\alpha \in [0, 1]$.

An explicit expression for the lower bound (5) in terms of the parameters ℓ , p , q , and α is given in the appendix.

Further, define

$$\begin{aligned} U &\stackrel{\text{def}}{=} \frac{p \cdot (\ell - 1) + q \cdot \log(2^{\ell+1} - 2)}{\ell} \\ &\quad + \frac{(1 - p - q) \log \sum_{x^\ell \in \{0,1\}^\ell} 2^{-\frac{p+q}{1-p-q} \hat{H}(\mathbf{r}(x^\ell))}}{\ell}, \end{aligned} \quad (7)$$

where $\hat{H}(\mathbf{r}(x^\ell))$ is the runlength empirical entropy of x^ℓ

$$\hat{H}(\mathbf{r}(x^\ell)) \stackrel{\text{def}}{=} - \sum_{i \geq 1} \frac{r_i(x^\ell)}{\ell} \log \frac{r_i(x^\ell)}{\ell}.$$

Proposition 1. For any $p, q, \alpha \in [0, 1]$ such that $p + q \leq 1$ and any integer $\ell > 1$, we have

$$L_{SI}^\alpha \leq C_{SI} \leq U. \quad (8)$$

In Fig. 1,

$$\Delta_{U, C_{SI}}(\ell) \stackrel{\text{def}}{=} \max_{p, q: p+q \leq 1} \frac{U - C_{SI}}{C_{SI}} \quad (9)$$

³Notice that $\sum_i r_i(\mathbf{x}) = |\mathbf{x}|$.

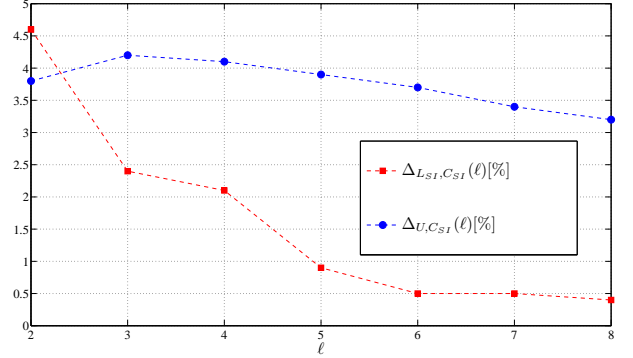


Fig. 1. Relative differences between C_{SI} and its upper bound U (given by $\Delta_{U, C_{SI}}(\ell)$) and between C_{SI} and its lower bound $\max_\alpha L_{SI}^\alpha$ (given by $\Delta_{L_{SI}, C_{SI}}(\ell)$).

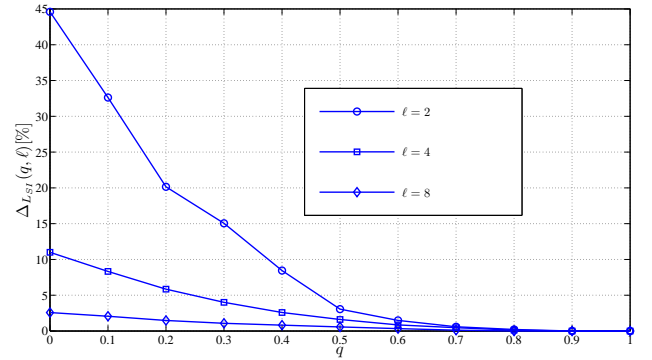


Fig. 2. Relative difference between $\max_\alpha L_{SI}^\alpha$ and $L_{SI}^{0.5}$.

and

$$\Delta_{L_{SI}, C_{SI}}(\ell) \stackrel{\text{def}}{=} \max_{p, q: p+q \leq 1} \frac{C_{SI} - \max_\alpha L_{SI}^\alpha}{C_{SI}} \quad (10)$$

represent the relative difference between C_{SI} , which is obtained numerically by the Arimoto-Blahut algorithm, and the upper and lower bounds U and L_{SI}^α , respectively, the latter being numerically optimized over $\alpha \in [0, 1]$.

As we can see, these bounds are fairly close for a wide range of p and q . For instance, their difference with respect to C_{SI} is at most 5% for any p and q such that $p + q \leq 0.6$, as long as $\ell \geq 2$. Moreover, numerical evidence suggests that both $\Delta_{U, C_{SI}}(\ell)$ and $\Delta_{L_{SI}, C_{SI}}(\ell)$ tend to zero as $\ell \rightarrow \infty$.

In Fig. 2

$$\Delta_{L_{SI}}(q, \ell) \stackrel{\text{def}}{=} \max_{p \in [0, 1-q]} \frac{\max_{\alpha \in [0, 1]} L_{SI}^\alpha - L_{SI}^{0.5}}{\max_{\alpha \in [0, 1]} L_{SI}^\alpha} \quad (11)$$

represents the relative difference between $L_{SI}^{0.5}$ and the optimized lower bound expression $\max_\alpha L_{SI}^\alpha$ as a function of q , for different values of ℓ . As we observe, when either ℓ or q decreases, non-uniform inputs perform significantly better than uniform inputs.

We now turn to the case where there is no side information at the receiver. For comparing our results with related work, we restrict ourselves to the purely deletion case, *i.e.*, $q = 0$.

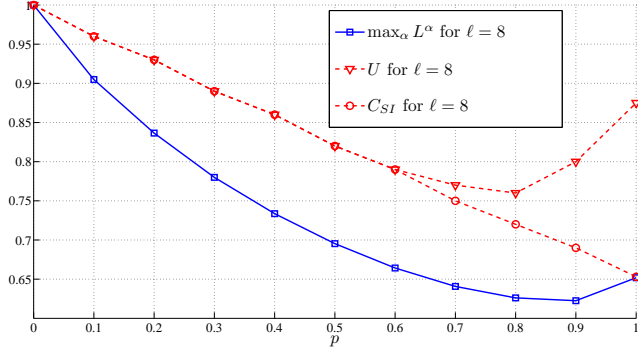


Fig. 3. Upper and lower bounds on the capacity of segmented deletion channel for $\ell = 8$.

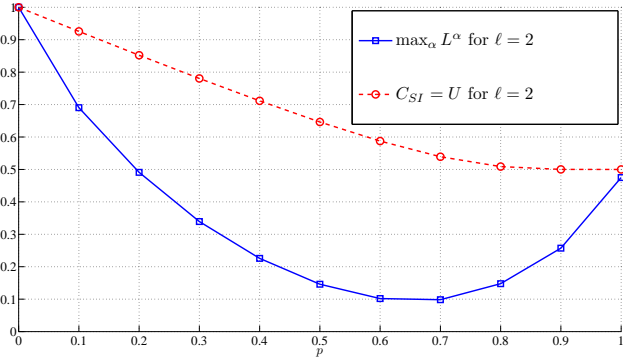


Fig. 4. Upper and lower bounds on the capacity of segmented deletion channel for $\ell = 2$.

For this channel, a lower bound to capacity is obviously

$$L^\alpha \stackrel{\text{def}}{=} L_{SI}^\alpha - H_b(p, q)/\ell$$

by (4) and (8).

Figures 3 and 4 represent the upper and lower bounds on C given by U and $\max_\alpha L^\alpha$ for $\ell = 8$ and $\ell = 2$, respectively. The difference between these bounds is particularly significant for $p \approx 1/2$. Indeed, this is partly due to the fact that the difference between the two bounds is lower by the side information $H_b(p, 0)/\ell$ which is maximal for $p = 1/2$. Also note that U may be better or worse than the numerical upper bound given in [14]. For instance, for $\ell = 8$ (Fig. 3) we have that U is lower than the upper bound proposed in [14] for $p \in [0, 0.6]$ whereas the opposite holds for $p \in (0.6, 1]$. Finally note that U appears to be a very good approximation for C_{SI} ; the difference gets negligible for $p \leq 0.6$ when $\ell = 8$ and is negligible for any $p \leq 1$ when $\ell = 2$.

Asymptotics

In the regime of large blocks and small synchronization errors we have:⁴

⁴We say that $f(\ell) = O(g(\ell))$ if there exists a positive real number k such that $|f(\ell)| \leq k \cdot g(\ell)$ when $\ell \rightarrow \infty$.

Theorem 1. i. For p and q such that $p + q \leq 1$, we have

$$L_{SI}^{0.5} = 1 - \frac{p+q}{\ell} \log \ell + \frac{p}{\ell}(K-1) + \frac{q}{\ell}(K+1) + (p+q)O(\ell^{-2}); \quad (12)$$

ii. When $(p+q) \log \ell \rightarrow 0$, we have

$$U = 1 - \frac{p+q}{\ell} \log \ell + \frac{p}{\ell}(K-1) + \frac{q}{\ell}(K+1) + O((p+q)^2(\log \ell)^2/\ell); \quad (13)$$

where $K = \sum_{j=1}^{\infty} \frac{j \log j}{2^{j+1}} \simeq 1.2885$.

iii. When $(p+q) \log \ell \rightarrow 0$, we have

$$C_{SI} = 1 - \frac{p+q}{\ell} \log \ell + \frac{p}{\ell}(K-1) + \frac{q}{\ell}(K+1) + (p+q)O(\ell^{-2}) + O\left(\frac{(p+q)^2}{\ell} \log^2 \ell\right). \quad (14)$$

We note that for $p = 1$ (and hence $q = 0$), the $1 - \frac{\log \ell}{\ell}$ term in (14) corresponds to the zero-error capacity of the one-bit purely deletion channel ([12, Theorem 2.5]).

Note that p and q do not play symmetric roles in the asymptotic capacity expression (14). An intuitive explanation for this is as follows. From the length of the output block the decoder knows whether the input to the channel experiences a deletion, a duplication, or remains unchanged. If a duplication occurs, then the decoder also knows the number of runs in the input since duplication cannot change the number of runs. By contrast, deletion errors can erase a run completely, thereby increasing decoding ambiguity. From Theorem 1 and (4), we readily obtain the following asymptotic expressions for the segmented deletion and duplication channel:

Corollary 1. i. For any p and q such that $p + q \leq 1$, we have

$$C = 1 - (p+q) \frac{\log \ell}{\ell} + O(\ell^{-1}); \quad (15)$$

ii. When $q = 0$ and $p = O(\ell^{-1})$ we have

$$L^{0.5} = 1 + (p/\ell) \log(p/\ell) - K_1 \cdot (p/\ell) + O(\ell^{-3}) \quad (16)$$

where $K_1 \stackrel{\text{def}}{=} \log(2e) - \sum_{j=1}^{\infty} \frac{j \log j}{2^{j+1}} \simeq 1.15416377$;

iii. When $p = 0$ and $q = O(\ell^{-1})$ we have

$$L^{0.5} = 1 + (q/\ell) \log(q/\ell) + K_2 \cdot (q/\ell) + O(\ell^{-3}) \quad (17)$$

where $K_2 \stackrel{\text{def}}{=} \sum_{j=1}^{\infty} \frac{j \log j}{2^{j+1}} - \log(e/2) \simeq 0.84583623$.

Note that the first three terms on the right-hand side of (16) correspond to the first terms in the asymptotic expansion of the capacity of the i.i.d. deletion channel with deletion probability p/ℓ .

III. PROOFS

We denote by p_d and p_i the unconditional probabilities of deletion and duplication, respectively, of each bit within a block of length ℓ , i.e.,

$$p_d \stackrel{\text{def}}{=} p/\ell \quad p_i \stackrel{\text{def}}{=} q/\ell.$$

Also, we denote by $n_r(\mathbf{x})$ the number of runs in a sequence \mathbf{x} .

⁵This constant appeared as A_1 in [7, Theorem 1].

A. Proof of Proposition 1

1) *Lower bound*: The left-hand side of (8) holds because of (3).

2) *Upper bound*: For any length ℓ output sequence \mathbf{y} , we have $P_Y(y^\ell) = (1-p-q)P_X(y^\ell)$ and $Q(y^\ell|x^\ell) = (1-p-q)$. For a length $\ell-1$ (respectively, $\ell+1$) output sequence \mathbf{y} , resulting from a one-bit deletion (respectively, duplication) in the i -th run of x^ℓ , we have $Q(\mathbf{y}|x^\ell) = \frac{p \cdot r_i}{\ell}$ (respectively, $\frac{q \cdot r_i}{\ell}$). Thus, we can write

$$\begin{aligned} I(X^\ell; \mathbf{Y}(X^\ell)) &= H(\mathbf{Y}(X^\ell)) - H(\mathbf{Y}(X^\ell)|X^\ell) \\ &= (1-p-q)H(X^\ell) \\ &+ (p+q) \sum_{\mathbf{x} \in \{0,1\}^\ell} P_X(\mathbf{x}) \sum_{i \in \{1, \dots, n_r(\mathbf{x})\}} \frac{r_i}{\ell} \cdot \log \frac{r_i}{\ell} \\ &- \sum_{|\mathbf{y}|=\ell-1} P_Y(\mathbf{y}) \log P_Y(\mathbf{y}) - \sum_{\mathbf{y}: |\mathbf{y}|=n_r(\mathbf{y})} P_Y(\mathbf{y}) \log P_Y(\mathbf{y}) \\ &+ p \log p + q \log q, \end{aligned} \quad (18)$$

The sum of the first two terms on the right-hand side of the second equality is a concave function of P_X . By the Lagrange multipliers method one deduces that the maximum is attained for the distribution

$$P_X^*(x^\ell) = \frac{2^{-\frac{p+q}{1-p-q} \hat{H}(\mathbf{r}(x^\ell))}}{\sum_{\mathbf{x} \in \{0,1\}^\ell} 2^{-\frac{p+q}{1-p-q} \hat{H}(\mathbf{r}(\mathbf{x}))}}.$$

Maximizing separately the third and the fourth terms on the right-hand side of the second equality in (18) under the constraints $\sum_{|\mathbf{y}|=\ell-1} P_Y(\mathbf{y}) = p$ and $\sum_{\mathbf{y}: |\mathbf{y}|=n_r(\mathbf{y})} P_Y(\mathbf{y}) = q$ is similar to entropy maximization and the maximums are achieved by the distributions

$$P_Y^{**}(y^{\ell-1}) = \frac{p}{2^{\ell-1}} \quad \text{and} \quad P_Y^{***}(y^{\ell+1}) = \frac{q}{2^{\ell+1}-2},$$

respectively.

Substituting distributions P_X^* , P_Y^{**} , and P_Y^{***} on the right-hand side of the second equality in (18) we obtain U .

B. Proof of Theorem 1

- i. This part of the theorem is obtained by deriving the asymptotic behavior of (27) as $\ell \rightarrow \infty$. To do this, we need the following lemma:

Lemma 1. *For any positive s, t such that $s+t=1$, we have:*

$$\begin{aligned} \sum_{k=1}^n \binom{n}{k} s^k t^{n-k} k \log k &= sn \log(sn) + t \log e + \frac{s-1}{2} \\ &+ O\left(\frac{1}{n}\right). \end{aligned} \quad (19)$$

Proof of Lemma 1: This lemma is proved via the moment generating function method of [5]. For any sequence of real numbers $\{f_k\}$, the Bernoulli transform of f_k is defined as

$$S_n \stackrel{\text{def}}{=} \sum_{k=0}^n \binom{n}{k} f_k s^k t^{n-k},$$

Further, for f_k and its Bernoulli transform S_n , the generating functions are defined by

$$f(z) \stackrel{\text{def}}{=} \sum_{k \geq 1} f_k z^k \quad \text{and} \quad S(z) \stackrel{\text{def}}{=} \sum_{n \geq 1} S_n z^n,$$

respectively.

It is easy to check (see [5]) that f and S satisfy

$$S(z) = \frac{1}{1-tz} f\left(\frac{sz}{1-tz}\right).$$

Now we consider two sequences of real numbers $f_k^{(1)} \stackrel{\text{def}}{=} \log k$ and $f_k^{(2)} \stackrel{\text{def}}{=} k \log k$, $k \geq 1$. For $f_k^{(i)}$ and $i \in \{1, 2\}$, we denote the Bernoulli transform, generating function, and generating function of the Bernoulli transform by $S_n^{(i)}$, $f^{(i)}(z)$, and $S^{(i)}(z)$, respectively. Also, we denote by g' the first derivative of a function g .

It is easy to check that $f^{(2)}(z) = z \cdot (f^{(1)})'(z)$ which implies that

$$S^{(2)}(z) = -tz S^{(1)}(z) + (1-tz)z(S^{(1)})'(z).$$

Now, from [5, Proposition 1], we know that

$$S_n^{(1)} = \log sn + \frac{s-1}{2sn} + O\left(\frac{1}{n^2}\right).$$

Denote by $[z^n]A(z)$ the n -th coefficient of a generating function $A(z)$. Since $[z^n]z^k S(z) = S_{n-k}$ and $[z^n]S'(z) = (n+1)S_{n+1}$, we obtain

$$\begin{aligned} S_n^{(2)} &= -t[\log(s(n-1)) + \frac{s-1}{2s(n-1)} + O(\frac{1}{n^2})] \\ &+ n[\log(sn) + \frac{s-1}{2sn} + O(\frac{1}{n^2})] \\ &- t(n-1)[\log s(n-1) + \frac{s-1}{2s(n-1)} + O(\frac{1}{n^2})] \\ &= sn \log(sn) + t \log e + \frac{s-1}{2} + O\left(\frac{1}{n}\right). \end{aligned}$$

Since $S_n^{(2)}$ corresponds to the left-hand side of (19) the proof is complete. ■

For any p and q , as $\ell \rightarrow \infty$, we have

$$\begin{aligned} \frac{p+q}{\ell^2} \sum_{j=1}^{\ell-1} \frac{\ell-j+3}{2^{j+1}} j \log j \\ = \frac{(p+q)K}{\ell} + (p+q)O(\ell^{-2}), \end{aligned} \quad (20)$$

where K is defined as

$$K \stackrel{\text{def}}{=} \lim_{\ell \rightarrow \infty} \sum_{j=1}^{\ell} 2^{-(j+1)} j \log j.$$

Also, we have

$$\begin{aligned}
& \frac{q}{\ell^2 \cdot 2^{\ell-1}} \sum_{m=1}^{\ell} m \binom{\ell}{m} \log m \\
&= \frac{2 \cdot q}{\ell^2} \sum_{m=1}^{\ell} (0.5)^m (0.5)^{\ell-m} \binom{\ell}{m} m \log m \\
&\stackrel{a}{=} \frac{2 \cdot q}{\ell^2} \left[\frac{\ell}{2} \log \frac{\ell}{2} \right] + q O(\ell^{-2}) \\
&= -\frac{q}{\ell} + \frac{q}{\ell} \log \ell + q O(\ell^{-2}), \tag{21}
\end{aligned}$$

where a follows from Lemma 1 by setting $s = t = 0.5$. By substituting (20) and (21) into (27) we obtain (12).

- ii. Since the runlengths of a length ℓ sequence are between 1 and ℓ , we have $\hat{H}(r(x^\ell)) \leq \log \ell$. If we assume that $(p+q) \log \ell \rightarrow 0$, we can use Taylor's expansion of 2^{-x} around $x = 0$ to get

$$\begin{aligned}
2^{-\frac{p+q}{1-p-q} \hat{H}(r(x^\ell))} &= 1 - \frac{(p+q)}{(1-p-q) \log e} \hat{H}(r(x^\ell)) \\
&\quad + O((p+q)^2 \ell^2). \tag{22}
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\sum_{x^\ell} 2^{-\frac{p+q}{1-p-q} \hat{H}(r(x^\ell))} &= 2^\ell (1 - O((p+q)^2 \ell^2)) \\
&\quad - \frac{(p+q)}{(1-p-q) \log e} \sum_{x^\ell} \hat{H}(r(x^\ell)). \tag{23}
\end{aligned}$$

Now, we establish the asymptotic behavior of $\sum_{x^\ell} \hat{H}(r(x^\ell))$. Denoting by $n(\ell, j)$, the number of times a run with length of j appears in all length ℓ sequences, we have

$$\begin{aligned}
\sum_{x^\ell} \hat{H}(r(x^\ell)) &= - \sum_{j=1}^{\ell} n(\ell, j) \frac{j}{\ell} \log \left(\frac{j}{\ell} \right) \\
&\stackrel{a}{=} - \sum_{j=1}^{\ell-1} 2^{\ell-j-1} \frac{\ell-j+3}{\ell} j \log \frac{j}{\ell} \\
&= -2^\ell \left(\sum_{j=1}^{\ell-1} 2^{-j-1} \frac{\ell-j+3}{\ell} j \log j \right. \\
&\quad \left. - \log(\ell) \cdot \sum_{j=1}^{\ell-1} 2^{-j-1} \frac{\ell-j+3}{\ell} j \right) \\
&\stackrel{b}{=} 2^\ell (\log \ell - K), \tag{24}
\end{aligned}$$

where a follows from [11, Proposition 2] and where b follows from $\sum_{j=1}^{\infty} \frac{j}{2^{j+1}} = 1$. Therefore, we have

$$\begin{aligned}
& \log \left(\sum_{x^\ell} 2^{-\frac{p+q}{1-p-q} \hat{H}(r(x^\ell))} \right) \\
&= \ell + \log \left(1 - \frac{p+q}{(1-p-q) \log 2} (\log \ell - K) \right) \\
&\quad + O(((p+q) \log \ell)^2)) \\
&= \ell - \frac{p+q}{1-p-q} (\log \ell - K) + O(((p+q) \log \ell)^2). \tag{25}
\end{aligned}$$

By substituting (25) in (7), we obtain (13).

- iii. The capacity expansion in (14) follows from (12), (13).

C. Proof of Corollary 1

- i. Since $\frac{H_b(p,q)}{\ell} = O(\ell^{-1})$, we have

$$L^{0.5} = 1 - \frac{(p+q) \log \ell}{\ell} + O(\ell^{-1}).$$

Also (2), (8), (13) imply that C is upper bounded by $1 - \frac{(p+q) \log \ell}{\ell} + O(\ell^{-1})$. The proof is complete.

- ii. We expand $(1-p) \log(1-p)$ around $p = 0$ to obtain

$$\begin{aligned}
L^{0.5} &= 1 - \frac{p}{\ell} \log \ell - \frac{p}{\ell} + \frac{p}{\ell} \log \left(\frac{p}{\ell} \right) + \left(\frac{p}{\ell} \right) K \\
&\quad + \frac{(1-p)}{\ell} (-p + O(p^2)) \log e + p O(\ell^{-2}) \\
&= 1 + p_d \log p_d - (\log 2e - K) p_d + O(\ell^{-3}).
\end{aligned}$$

- iii. The proof is similar to the previous case.

REFERENCES

- [1] S. Diggavi and M. Grossglauser, On information transmission over a finite buffer channel, *IEEE Trans. Inform. Theory*, 52:52, 2006.
- [2] R. L. Dobrushin, Shannon theorems for channels with synchronization errors, *Problemy Peredachi Informatsii*, pages 18–36, 1967.
- [3] E. Drinea and M. Mitzenmacher, Improved lower bounds for the capacity of i.i.d. deletion and duplication channels, *Information Theory, IEEE Transactions on*, 53(8):2693–2714, Aug. 2007.
- [4] D. Fertonani and T. M. Duman, Novel bounds on the capacity of the binary deletion channel. *Information Theory, IEEE Transactions on*, 56(6):2753–2765, June 2010.
- [5] P. Flajolet, Singularity Analysis and Asymptotics of Bernoulli Sums, *Rapport de recherche RR-3401*, INRIA, 1998.
- [6] Y. Kanoria and A. Montanari, On the deletion channel with small deletion probability, *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1002–1006, June 2010.
- [7] Y. Kanoria and A. Montanari, Optimal coding for the deletion channel with small deletion probability, *CoRR*, abs/1104.5546, 2011.
- [8] A. Kirsch and E. Drinea, Directly lower bounding the information capacity for channels with i.i.d. deletions and duplications, *Information Theory, IEEE Transactions on*, 56(1):86–102, Jan. 2010.
- [9] Z. Liu and M. Mitzenmacher, Codes for deletion and insertion channels with segmented errors, *IEEE Transaction on Information Theory*, 56(1):224–232, 2010.
- [10] R. Mahmoudvand, H. Hassani, A. Farzaneh, and G. Howell, The exact number of nonnegative integer solutions for a linear diophantine inequality, *IAENG International Journal of Applied Mathematics*, 40(1):1–5, 2010.
- [11] M. Rahmati and T. M. Duman, Analytical lower bounds on the capacity of insertion and deletion channels, *CoRR*, abs/1101.1310, 2011.
- [12] N. J. A. Sloane, On single-deletion-correcting codes, *Ohio State University*, pages 273–291, 2001.
- [13] R. Venkataramanan, S. Tatikonda, and K. Ramchandran, Achievable rates for channels with deletions and insertions, *CoRR*, abs/1102.5112, 2011.
- [14] F. Wang, D. Aktas, and T. M. Duman, On capacity and coding for segmented deletion channels, *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, pages 1408–1413, sept. 2011.

APPENDIX

For any $p, q, \alpha \in [0, 1]$ such that $p + q \leq 1$, and any integer $\ell > 1$ we have

$$\begin{aligned}
 L_{SI}^\alpha = & \frac{1 + (1-p)(\ell-1)H_b(\alpha) + (p+q)(1-\alpha)^{\ell-1} \log \ell}{\ell} \\
 & - \frac{p}{\ell^2(1-\alpha)} \left[\left(2\alpha^3(\ell-2) - (\ell^2 + \ell - 6)\alpha^2 \right. \right. \\
 & \quad \left. \left. + (\ell^2 - 3\ell - 2)\alpha + 2\ell \right) \log \alpha \right. \\
 & \quad \left. + \left(-2\alpha^3(\ell-2) + \alpha^2(\ell^2 + \ell - 6) \right. \right. \\
 & \quad \left. \left. - 2\alpha(\ell^2 - 2\ell - 1) + \ell(\ell-3) \right) \log(1-\alpha) \right] \\
 & - \frac{p\alpha^2(1-\alpha)^{\ell-3}}{\ell^2} \sum_{m=0}^{\ell-2} \left[\binom{\ell-2}{m} (\beta + \gamma + \gamma m) \times \right. \\
 & \quad \left. \left(\frac{\alpha}{1-\alpha} \right)^m \log(\beta + \gamma + \gamma m) \right] \\
 & - \frac{q\alpha^\ell}{\ell^2(1-\alpha)} \sum_{m=1}^{\ell} \binom{\ell}{m} \left(\frac{\alpha}{1-\alpha} \right)^{-m} m \log m \\
 & + \frac{p+q}{\ell^2} \sum_{m=2}^{\ell} m\alpha^{m-1}(1-\alpha)^{\ell-m} \times \\
 & \quad \left(\sum_{k=1}^{\ell-m+1} \binom{\ell-k-1}{m-2} k \log k \right), \quad (26)
 \end{aligned}$$

where

$$\gamma \stackrel{\text{def}}{=} \frac{1-2\alpha}{\alpha^2} \quad \text{and} \quad \beta \stackrel{\text{def}}{=} \frac{\ell-1 + (\alpha^2 - \alpha)(2\ell-4)}{\alpha^2}.$$

When $\alpha = 1/2$ the above expression reduces to

$$\begin{aligned}
 L_{SI}^{0.5} = & 1 - \frac{p}{\ell} - \frac{q}{\ell^2 \cdot 2^{\ell-1}} \sum_{m=1}^{\ell} m \binom{\ell}{m} \log m \\
 & - \left(p - \frac{p+q}{2^{\ell-1}} \right) \frac{\log \ell}{\ell} \\
 & + \frac{p+q}{\ell^2} \sum_{j=1}^{\ell-1} \frac{(\ell-j+3)}{2^{j+1}} \times j \log j. \quad (27)
 \end{aligned}$$

Proof: In order to prove (26), we need the following lemmas.

Lemma 2. For any integer $n \geq 1$, we have

$$\begin{aligned}
 \sum_{k=0}^n \binom{n}{k} k \cdot t^k &= n(1+t)^{n-1}t \\
 \sum_{k=0}^n \binom{n}{k} k^2 \cdot t^k &= n(1+t)^{n-1}t + n(n-1)(1+t)^{n-2}t^2. \quad (28)
 \end{aligned}$$

Proof of Lemma 2: The first and second equations can be obtained by taking the first and second derivatives with respect to t of the Binomial equation

$$\sum_{k=0}^n \binom{n}{k} t^k = (1+t)^n.$$

Lemma 3. • The number of length ℓ sequences containing m runs is

$$n'(\ell, m) = 2 \binom{\ell-1}{m-1}. \quad (29)$$

• The number of length k runs among all length ℓ sequences containing m runs is

$$n''(k, m, \ell) = \begin{cases} 2 & \text{if } m=1, k=\ell \\ 2m \binom{\ell-k-1}{m-2} & \text{if } m \geq 2, k \leq \ell-m+1 \\ 0 & \text{otherwise} \end{cases} \quad (30)$$

Proof of Lemma 3:

• The number of length ℓ sequences containing m runs is twice the number of positive integer solutions of equation

$$r_1 + \dots + r_m = \ell \quad (31)$$

which is [10]

$$\binom{\ell-1}{m-1}.$$

• Since the only two sequences containing 1 run are the all-zero and all-one sequences we have $n''(\ell, 1, \ell) = 2$. The number of runs of length k among all length ℓ sequences containing m runs is twice the number of times k appears in the solution set of (31). The number of times that the first run has length k is twice the number of positive integer solutions of $r_2 + \dots + r_m = \ell - k$. Therefore, the number of times a run of length k appears in all length ℓ sequences containing m runs is equal to $2m \binom{\ell-k-1}{m-2}$. ■

We write L_{SI}^α as

$$L_{SI}^\alpha = \frac{H(\tilde{\mathbf{Y}}) - H(\tilde{\mathbf{Y}}|X^\ell(\alpha))}{\ell}.$$

First, we calculate $H(\tilde{\mathbf{Y}}|X^\ell(\alpha))$. To compute this entropy, we need to calculate the probabilities of all output sequences. We classify the output sequences according to their lengths. For length ℓ sequences, we have

$$P_Y(y^\ell) = (1-p-q)P_X(y^\ell),$$

which results in

$$\begin{aligned}
 - \sum_{y^\ell} P_Y(y^\ell) \log P_Y(y^\ell) &= (1-p-q)H(X^\ell(\alpha)) \\
 &\quad - (1-p-q) \log(1-p-q) \quad (32)
 \end{aligned}$$

where the input block entropy is given by

$$H(X^\ell(\alpha)) = 1 + (\ell-1)H_b(\alpha). \quad (33)$$

Now, we turn to output sequences of length $\ell-1$. For any $\alpha \in [0, 1]$ and integers $\ell \geq 1$ and $m \leq \ell$, we define

$$f(\ell, m, \alpha) \stackrel{\text{def}}{=} 0.5(1-\alpha)^{\ell-m-1}\alpha^m. \quad (34)$$

The probability of any sequence generated by a first-order Markov process is a function of the number of its transitions.⁶ Since the number of transitions of a sequence \mathbf{x} is equal to $n_r(\mathbf{x}) - 1$, for any length ℓ sequence generated by (6), we can write

$$P_X(\mathbf{x}) = f(\ell, n_r(\mathbf{x}) - 1, \alpha). \quad (35)$$

To calculate $P_Y(y^{\ell-1})$, we need to calculate the probability of each of its length ℓ super-sequences.⁷ A length ℓ super-sequence of \mathbf{y} can be generated by inserting one bit into $y^{\ell-1}$ in one of the following ways:

- Insert one zero (one) to one of its runs of zeros (ones). The number of distinct super-sequences generated under this scenario is equal to $n_r(\mathbf{y})$. Let \mathbf{x}' be sequence \mathbf{y} with one bit inserted in its i -th run. Hence we have $Q(\mathbf{y}|\mathbf{x}') = (r_i(\mathbf{y}) + 1) \cdot p_d$. Also, note that for any such \mathbf{x}' we have $n_r(\mathbf{y}) = n_r(\mathbf{x}')$ and thus, $P_X(\mathbf{x}') = f(\ell, n_r(\mathbf{y}) - 1, \alpha)$.
- Insert one opposite bit at one of its ends. The number of possible super-sequences generated under this scenario is 2. For any such super-sequences \mathbf{x}'' we have $Q(\mathbf{y}|\mathbf{x}'') = p_d$. Also, note that $n_r(\mathbf{x}'') = n_r(\mathbf{y}) + 1$ and thus $P_X(\mathbf{x}'') = f(\ell, n_r(\mathbf{y}), \alpha)$.
- Insert one opposite bit inside of one of its runs. Since for any sequence of length $\ell - 1$, there are $\ell + 1$ super-sequences of length ℓ , the number of possible super-sequences generated under this scenario is $\ell - n_r(\mathbf{y}) - 1$. For any such \mathbf{x}''' we have $Q(\mathbf{y}|\mathbf{x}''') = p_d$ and $P_X(\mathbf{x}''') = f(\ell, n_r(\mathbf{y}) + 1, \alpha)$.

Therefore, for any $\mathbf{y} \in \{0, 1\}^{\ell-1}$, we have

$$\begin{aligned} P_Y(\mathbf{y}) &= \sum_{x^\ell} P_X(x^\ell) Q(\mathbf{y}|x^\ell) \\ &= (\beta + \gamma \cdot n_r(\mathbf{y})) f(\ell, n_r(\mathbf{y}) + 1, \alpha) p_d. \end{aligned} \quad (36)$$

Hence, we have

$$\begin{aligned} & - \sum_{\mathbf{y} \in \{0, 1\}^{\ell-1}} P_Y(\mathbf{y}) \log P_Y(\mathbf{y}) \\ &= -(p_d \log p_d) \sum_{\mathbf{y}} (\beta + \gamma \cdot n_r(\mathbf{y})) f(\ell, n_r(\mathbf{y}) + 1, \alpha) \\ & \quad - p_d \sum_{\mathbf{y}} (\beta + \gamma \cdot n_r(\mathbf{y})) f(\ell, n_r(\mathbf{y}) + 1, \alpha) \times \\ & \quad \log [(\beta + \gamma \cdot n_r(\mathbf{y})) f(\ell, n_r(\mathbf{y}) + 1, \alpha)] \\ &= -(p_d \log p_d) \cdot A_1 - p_d \cdot (A_2 + A_3), \end{aligned} \quad (37)$$

where

$$\begin{aligned} A_1 &\stackrel{\text{def}}{=} \sum_{\mathbf{y}} (\beta + \gamma \cdot n_r(\mathbf{y})) f(\ell, n_r(\mathbf{y}) + 1, \alpha) \\ &= \ell, \end{aligned} \quad (38)$$

⁶Number of transitions of a sequence is the number of times its two consecutive bits differ

⁷ \mathbf{x} is super-sequence of \mathbf{y} if \mathbf{y} is a subsequence of \mathbf{x}

$$\begin{aligned} A_2 &\stackrel{\text{def}}{=} \sum_{m=1}^{\ell-1} \left[n'(\ell-1, m) (\beta + \gamma m) f(\ell, m+1, \alpha) \times \right. \\ & \quad \left. \log(\beta + \gamma m) \right] \\ &= \alpha^2 (1-\alpha)^{\ell-3} \sum_{m=0}^{\ell-2} \left[\binom{\ell-2}{m} (\beta + \gamma + \gamma m) \times \right. \\ & \quad \left. \left(\frac{\alpha}{1-\alpha} \right)^m \log(\beta + \gamma + \gamma m) \right], \end{aligned} \quad (39)$$

$$\begin{aligned} A_3 &\stackrel{\text{def}}{=} \sum_{m=1}^{\ell-1} \left[\binom{\ell-2}{m-1} (\beta + \gamma m) (1-\alpha)^{\ell-m-2} \alpha^{m+1} \right. \\ & \quad \left. \times \log(0.5(1-\alpha)^{\ell-m-2} \alpha^{m+1}) \right] \\ &= B_1 + B_2 - B_3, \end{aligned} \quad (40)$$

with

$$\begin{aligned} B_1 &\stackrel{\text{def}}{=} \alpha (1-\alpha)^{\ell-2} \log \alpha \times \\ & \quad \sum_{m=1}^{\ell-1} \left[\binom{\ell-2}{m-1} (\beta + \gamma m) \times \left(\frac{\alpha}{1-\alpha} \right)^m (m+1) \right] \\ &= \frac{\log \alpha}{1-\alpha} [2\alpha^3(\ell-2) - (\ell^2 + \ell - 6)\alpha^2 \\ & \quad + (\ell^2 - 3\ell - 2)\alpha + 2\ell], \end{aligned} \quad (41)$$

$$\begin{aligned} B_2 &\stackrel{\text{def}}{=} \alpha (1-\alpha)^{\ell-2} \log(1-\alpha) \times \\ & \quad \sum_{m=1}^{\ell-1} \left[\binom{\ell-2}{m-1} (\beta + \gamma m) \left(\frac{\alpha}{1-\alpha} \right)^m (\ell - m - 2) \right] \\ &= \frac{\log(1-\alpha)}{1-\alpha} [-2\alpha^3(\ell-2) + \alpha^2(\ell^2 + \ell - 6) \\ & \quad - 2\alpha(\ell^2 - 2\ell - 1) + \ell(\ell - 3)], \end{aligned} \quad (42)$$

$$\begin{aligned} B_3 &\stackrel{\text{def}}{=} \sum_{m=1}^{\ell-1} \left[\binom{\ell-2}{m-1} (\beta + \gamma m) (1-\alpha)^{\ell-m-2} \alpha^{m+1} \right] \\ &= \ell. \end{aligned} \quad (43)$$

Now, we consider the length $\ell+1$ output sequences. Obviously, for the alternating sequences (*i.e.*, \mathbf{y} such that $|\mathbf{y}| = n_r(\mathbf{y})$) of length $\ell+1$, we have $P_Y(\mathbf{y}) = 0$. Denoting by \mathcal{Y}^* the set of length $\ell+1$ non-alternating sequences, for any $\mathbf{y} \in \mathcal{Y}^*$ the duplicated bit can be found in one of the runs of \mathbf{y} with a length greater than 1. Hence, for any $\mathbf{y} \in \mathcal{Y}^*$, we have

$$\begin{aligned} P_Y(\mathbf{y}) &= \sum_{j: r_j(\mathbf{y}) > 1} (r_j(\mathbf{y}) - 1) p_i \cdot f(\ell, n_r(\mathbf{y}) - 1, \alpha) \\ &= (\ell + 1 - n_r(\mathbf{y})) p_i \cdot f(\ell, n_r(\mathbf{y}) - 1, \alpha), \end{aligned}$$

where the second equality follows from the fact that duplication error can not create a new run in the received sequence.

Thus, we have

$$\begin{aligned}
& - \sum_{\mathbf{y} \in \mathcal{Y}^*} P_Y(\mathbf{y}) \log P_Y(\mathbf{y}) = q(1 - \log q) + q(\ell - 1)H_b(\alpha) \\
& + q \log \ell - \frac{q}{\ell} \frac{\alpha^\ell}{1 - \alpha} \sum_{m=1}^{\ell} \binom{\ell}{m} \left(\frac{\alpha}{1 - \alpha} \right)^{-m} m \log m.
\end{aligned} \tag{44}$$

Now, we turn to $H(\mathbf{Y}(X^\ell)|X^\ell)$. We have

$$\begin{aligned}
H(\mathbf{Y}(X^\ell)|X^\ell) &= H_b(p, q) + (p + q) \log \ell \\
& - \frac{p + q}{\ell} \sum_{\mathbf{x} \in \{0,1\}^\ell} P_X(\mathbf{x}) \sum_{i=1}^{n_r(\mathbf{x})} r_i(\mathbf{x}) \log r_i(\mathbf{x}).
\end{aligned} \tag{45}$$

Denoting by $n''(k, m, \ell)$ the number of times a run of length k appears in all possible length ℓ sequences containing m runs

we have

$$\begin{aligned}
& \sum_{\mathbf{x} \in \{0,1\}^\ell} P_X(\mathbf{x}) \sum_{i=1}^{n_r(\mathbf{x})} r_i(\mathbf{x}) \log r_i(\mathbf{x}) \\
&= \sum_{m=1}^{\ell} \sum_{\mathbf{x}: n_r(\mathbf{x})=m} P_X(\mathbf{x}) \sum_{i=1}^{n_r(\mathbf{x})} r_i(\mathbf{x}) \log r_i(\mathbf{x}) \\
&= \sum_{m=1}^{\ell} f(\ell, \alpha, m - 1) \sum_{\mathbf{x}: n_r(\mathbf{x})=m} \sum_{i=1}^m r_i(\mathbf{x}) \log r_i(\mathbf{x}) \\
&= \sum_{m=1}^{\ell} f(\ell, \alpha, m - 1) \sum_{k=1}^{\ell-m+1} n''(k, m, \ell) \cdot k \log k \\
&= \sum_{m=2}^{\ell} m f(\ell, \alpha, m - 1) \sum_{k=1}^{\ell-m+1} 2 \binom{\ell - k - 1}{m - 2} \cdot k \log k \\
& \quad + (1 - \alpha)^{\ell-1} \ell \log \ell
\end{aligned} \tag{46}$$

where the last equality follows from Lemma 3. Putting (36), (37), (38), (39), (40), (41), (42), (43), (44), (45), (46) together, we get L_{SI}^α . ■